



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/549,885

09/16/2005

Claudine Viegas Conrado

NL 030293

7551

24737

7590

03/09/2009

PHILIPS INTELLECTUAL PROPERTY & STANDARDS

P.O. BOX 3001

BRIARCLIFF MANOR, NY 10510

EXAMINER

SQUIRES, BRETT S

ART UNIT

PAPER NUMBER

2431

MAIL DATE

DELIVERY MODE

03/09/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/549,885	<b>Applicant(s)</b> CONRADO ET AL.	
	<b>Examiner</b> BRETT SQUIRES	<b>Art Unit</b> 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 19 November 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-10 and 12-32 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10 and 12-32 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 19 November 2008 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

***Claim Rejections - 35 USC § 103***

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-2, 5-9, 12-19, 22-26, and 29-32 are rejected under 35 U.S.C. 103(a) as being obvious over Saito et al. ("Privacy Enhanced Access Control by SPKI") in view of Micall (US 5,717,758).

Regarding Claims 1-2, 5, and 12-13:

Saito discloses a privacy enhanced access control by simple public key infrastructure that associates user identifying information ("An Identity" See page 301 section I.) and data ("Authorization Field of the SPKI Certificate" See pages 302-303) that conceals a user identity using concealing data ("Public Key of the subject in the SPKI certificate," See pages 302-303 section II. B1.) in the user identifying information, wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.), such that it is possible to check for a given user identity whether the association applies to it ("In a sense, this public key is a kind of disposable fingerprint: it isn't identical with ID, but it is a proof the client." See page 303 section II. C.).

Saito does not disclose reissuing associations between user identifying information and data.

Art Unit: 2431

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claims 6-8:

Saito discloses an issuing agent (See figure 5 ref. no. A) receives a request for an association from a client (See figure 5 ref. no. C) and the issuing agent provides an association signed by its own secret key to the client (See pages 304-305 Section III. B.).

Regarding Claim 14:

Saito discloses the privacy enhanced access control by simple public key infrastructure operates in internet and electronic commerce applications (See page 301 abstract). The examiner respectfully points out that pay per access content is available on the internet in electronic commerce applications.

Regarding Claim 15:

Saito discloses the authorization field of the SPKI Certificate has a content identifier ("File1, File2" See pages 302-303 section II. B1.)

Regarding Claim 16:

Saito discloses the SPKI Certificate includes a rights attributes data field ("Validity" See pages 302-303 section II. B1.).

Regarding Claims 18-19:

Saito discloses sending a request in relation to the data including the concealed user identifying information ("Exercise and Service communication between the Server and the Client" See figure 5 and page 305 section III. B.).

Regarding Claims 22-25:

Saito discloses privacy enhanced access control by simple public key infrastructure that receives from a user a request concerning the data using user identifying information related to the user ("SPKI S' Certificate" and "SPKI A' Certificate" See figure 5 and pages 303-305 section III.), retrieves the association including user identifying information that has been concealed using concealing data ("Exercise" See pages 304-305 section III. B.) wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.), checks the concealed user identifying information in the association ("Exercise" See pages 304-305 section III. B.), and provides the user with information related to the data based on a correspondence between the concealed user identifying information in the association and the user identifying information at least linked to the user ("Exercise" and "Service" See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 26:

Saito discloses comparing the user identifying information of the user against a user domain certificate ("SPKI S' Certificate" See figure 5 and pages 304-305 section III. B.) including user identifying information related to all users in a domain ("The examiner respectfully points out that the amount of users in a domain can be as few as one."), wherein the step of checking concealed user identifying information in the association with user identifying information is performed on user identifying information in the domain certificate ("SPKI S' Certificate" and "SPKI A' Certificate" See figure 5 and pages 304-305 section III. B.), and the step of providing is performed based on a correspondence between the concealed user identifying information in the association and any user identifying information in the domain certificate ("Secure Downloading" See pages 304-305 section III. B.).

Regarding Claim 29:

Saito discloses a privacy enhanced access control by simple public key infrastructure that conceals user identifying information ("An Identity" See page 301

Art Unit: 2431

section I.) in an association between a user and data ("Authorization Field of the SPKI Certificate" See pages 302-303) using concealing data ("Public Key of the subject in the SPKI certificate," See pages 302-303 section II. B1.) for provision of the concealed user identifying information in the association, wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.)

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 30:

Saito discloses a privacy enhanced access control by simple public key infrastructure that receives a request ("Exercise" See pages 304-305 section III. B.) from a user to access information in relation to an association between the user and, the data including user identifying information relating to the user ("SPKI A' Certificate" See figure 5 and pages 303-305 section III.), retrieve an association between the data and a user including user identifying information which has been concealed using

Art Unit: 2431

concealing data ("Subject Field of the SPKI Certificate" and "Authorization Field of the SPKI Certificate" See pages 302-303 Section II.), wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.), check the concealed user identifying information in the association ("The server verifies the properness of certificates," See pages 304-305 section III. B.), provide the user with information related to the data based on a correspondence between the concealed user identifying information in the association and user identifying information at least linked to the user ("Secure Downloading" See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 31:

Saito discloses a privacy enhanced access control by simple public key infrastructure that receives user identifying information related to a user ("SPKI S' Certificate" and "SPKI A' Certificate" See figure 5 and pages 303-305 section III.), the



Art Unit: 2431

user identifying information being relation to an association between the user and data ("Authorization Field of the SPKI Certificate" See pages 302-303), identifying information is concealed using concealing data ("Public Key of the subject in the SPKI certificate," See pages 302-303 section II. B1.), send a request concerning that data including the concealed user identifying information ("Exercise" See figure 5 ref. no. 4 and page 305), wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.), so that the association between the user and the data comprising the concealed user identifying information can be received ("The server verifies the properness of certificates," See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

Regarding Claim 32:

Saito discloses a privacy enhanced access control by simple public key infrastructure that receives a request ("Exercise" See figure 5 ref. no. 4 and page 305)

Art Unit: 2431

concerning the data including the user identifying information which has been concealed using concealing data ("Public Key of the subject in the SPKI certificate," See pages 302-303 section II. B1.), the data being included in an association between the user and the data ("Authorization Field of the SPKI Certificate" See pages 302-303), wherein the concealing data remains fixed for a set time period ("The validity field defines how the certificate is valid, for example a period of time." See pages 302-303 section II. B1.), and provide the association between the user and the data comprising the concealed user identifying information ("The server verifies the properness of certificates," See pages 304-305 section III. B.).

Saito does not disclose reissuing associations between user identifying information and data.

Micall discloses reissuing valid certificates (See col. 5 lines 55-67 and col. 6 lines 1-20).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the privacy enhanced access control by simple public key infrastructure to include reissuing valid SPKI certificates such as that taught by Micall in order reduce processing overhead by reissuing a valid certificate instead of generating a new certificate.

3. Claims 3-4, 10, 20-21, 27-28 are rejected under 35 U.S.C. 103(a) as being obvious over Saito et al. ("Privacy Enhanced Access Control by SPKI") in view of Micall (US 5,717,758) further in view of Alldredge (US 2007/0189542).

Art Unit: 2431

Regarding Claims 3 and 10:

Saito discloses the above stated privacy enhanced access control by simple public key infrastructure that conceals a user identity using a hash function.

Saito does not disclose concealing a user identity using encryption.

Allredge discloses a cryptographic system that encrypts a users message using a symmetric key (See paragraph 7).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the privacy enhanced access control by simple public key infrastructure symmetric key based encryption such as that taught by Allredge in order to achieve privacy between a message sender and a message receiver (See Allredge paragraph 7).

Regarding Claim 4:

Saito discloses the above stated privacy enhanced access control by simple public key infrastructure that conceals a user identity using a hash function.

Saito does not disclose the concealing data includes a random value.

Allredge discloses a method for secured electronic commerce using sequences of one time pads for concealing transmitted messages (See paragraphs 25 and 60)

It would have been obvious to one of ordinary skill in the art at the time of the invention to included in the privacy enhanced access control by simple public key infrastructure concealing transmitted messages using one time pads such as that taught by Allredge in order to allow the privacy enhanced access control by simple public key infrastructure to be used internationally (See paragraph 19).

Art Unit: 2431

Regarding Claims 20-21 and 27-28:

Saito discloses the above stated privacy enhanced access control by simple public key infrastructure sending a request in relation to the data including the concealed user identifying information.

Saito does not disclose the request includes a secret security identifier and encrypting the concealing data using a secret domain key.

Allredge discloses a cryptographic system that includes a secret security identifier ("Symmetric Key" See paragraphs 10 and 11) with a message and encrypts the message containing the secret security identifier using secret domain key ("Recipient's Public Key" See paragraphs 10 and 11).

It would have been obvious to one of ordinary skill in the art at the time of the invention to include in the privacy enhanced access control by simple public key infrastructure a symmetric key system and an asymmetric key system such as those taught by Allredge in order to achieve privacy between a message sender and a message receiver (See Allredge paragraph 7).

### ***Response to Arguments***

4. Applicant's arguments filed November 19, 2008 with respect to claims 1-10 and 12-32 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRETT SQUIRES whose telephone number is (571) 272-8021. The examiner can normally be reached on 9:30am - 6:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2431

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BS/

/Christopher A. Revak/  
Primary Examiner, Art Unit 2431